WEST Search History

DATE: Monday, October 27, 2003

Set Name side by side	Query	Hit Count	Set Name result set
DB=USPT,PGPB,JPAB,EPAB,DWPI,TDBD; PLUR=YES; OP=ADJ			
L41	L40 and (rule or policy)	28	L41
L40	evaluat$ with (business or plan$) and vot$ not l39	67	L40
L39	evaluat$ near5 business and vot$	18	L39
L38	L19 not @ad>1995 and transaction	3	L38
L37	L19 not @py>1995 and transaction	30	L37
L36	L35 and transaction	189	L36
L35	L19 not @py<1995	539	L35
L34	L19 same transaction	47	L34
L33	L30 and L19 same transaction	0	L33
L32	L30 and transaction	0	L32
L31	L30 same transaction	0	L31
L30	L29 not l24	534	L30
L29	L19 not @ad<1984	747	L29
L28	l19 and @ad>=1984 and transaction	210	L28
L27	l19 not @ad>=1984 and transaction	3	L27
L26	l19 not @ad>=1984 same transaction	747	L26
L25	l19 not @ad<=1984 same transaction	747	L25
L24	l19 not @ad<=1984 and transaction	213	L24
L23	l22 and transaction	8	L23
L22	L19 not @py>1984	66	L22
L21	L20 not @py>1984	7	L21
L20	L19 and 1984	36	L20
L19	without near5 $card same (voice or print or imprint or eye$ or scan or fingerprint or iris or retinal or biometric) not l1 not l18 not l17	747	L19
DB=USPT; PLUR=YES; OP=ADJ			
L18	((without near5 $card) with transaction) same (voice or print or imprint or eye$ or scan or fingerprint or iris or retinal) not l1	3	L18
DB=USPT,PGPB,JPAB,EPAB,DWPI,TDBD; PLUR=YES; OP=ADJ			
L17	((without near5 card) with transaction) same (voice or print or imprint or eye$ or scan or fingerprint or iris or retinal) not l1	26	L17
DB=USPT; PLUR=YES; OP=ADJ			

L16	((without near5 card) with transaction) same (voice or print or imprint or eye$ or scan or fingerprint or iris or retinal) not l1	3	L16
DB=JPAB,EPAB,DWPI,TDBD; PLUR=YES; OP=ADJ			
L15	((without near5 card) near5 transaction) same biometric	1	L15
DB=USPT; PLUR=YES; OP=ADJ			
L14	L13 not l5	88	L14
L13	L12 not l8	88	L13
L12	L11 not l6	88	L12
L11	l1 not l4	125	L11
DB=USPT,PGPB; PLUR=YES; OP=ADJ			
L10	cardless near5 transaction	20	L10
DB=USPT; PLUR=YES; OP=ADJ			
L9	L8 not l3	1	L9
L8	L6 not l2	30	L8
L7	L6 not l2 not l3 not l4	0	L7
L6	L5 not l2-l4	38	L6
L5	l1 and retinal	38	L5
L4	l1 and (voice or print or imprint or eye$ or scan or fingerprint) not l3 not l2	118	L4
L3	l1 and biometric not l2	38	L3
L2	l1 same biometric	8	L2
L1	((without near5 card) near5 transaction)	243	L1

END OF SEARCH HISTORY

WEST Search History

DATE: Monday, October 27, 2003

Set Name side by side	Query	Hit Count	Set Name result set
DB=USPT,PGPB; PLUR=YES; OP=ADJ			
L10	cardless near5 transaction	20	L10
DB=USPT; PLUR=YES; OP=ADJ			
L9	L8 not l3	1	L9
L8	L6 not l2	30	L8
L7	L6 not l2 not l3 not l4	0	L7
L6	L5 not l2-l4	38	L6
L5	l1 and retinal	38	L5
L4	l1 and (voice or print or imprint or eye$ or scan or fingerprint) not l3 not l2	118	L4
L3	l1 and biometric not l2	38	L3
L2	l1 same biometric	8	L2
L1	((without near5 card) near5 transaction)	243	L1

END OF SEARCH HISTORY

WEST Search History

DATE: Monday, October 27, 2003

Set Name side by side	Query	Hit Count	Set Name result set
DB=USPT,PGPB,JPAB,EPAB,DWPI,TDBD; PLUR=YES; OP=ADJ			
L28	l19 and @ad>=1984 and transaction	210	L28
L27	l19 not @ad>=1984 and transaction	3	L27
L26	l19 not @ad>=1984 same transaction	747	L26
L25	l19 not @ad<=1984 same transaction	747	L25
L24	l19 not @ad<=1984 and transaction	213	L24
L23	l22 and transaction	8	L23
L22	L19 not @py>1984	66	L22
L21	L20 not @py>1984	7	L21
L20	L19 and 1984	36	L20
L19	without near5 $card same (voice or print or imprint or eye$ or scan or fingerprint or iris or retinal or biometric) not l1 not l18 not l17	747	L19
DB=USPT; PLUR=YES; OP=ADJ			
L18	((without near5 $card) with transaction) same (voice or print or imprint or eye$ or scan or fingerprint or iris or retinal) not l1	3	L18
DB=USPT,PGPB,JPAB,EPAB,DWPI,TDBD; PLUR=YES; OP=ADJ			
L17	((without near5 card) with transaction) same (voice or print or imprint or eye$ or scan or fingerprint or iris or retinal) not l1	26	L17
DB=USPT; PLUR=YES; OP=ADJ			
L16	((without near5 card) with transaction) same (voice or print or imprint or eye$ or scan or fingerprint or iris or retinal) not l1	3	L16
DB=JPAB,EPAB,DWPI,TDBD; PLUR=YES; OP=ADJ			
L15	((without near5 card) near5 transaction) same biometric	1	L15
DB=USPT; PLUR=YES; OP=ADJ			
L14	L13 not l5	88	L14
L13	L12 not l8	88	L13
L12	L11 not l6	88	L12
L11	l1 not l4	125	L11
DB=USPT,PGPB; PLUR=YES; OP=ADJ			
L10	cardless near5 transaction	20	L10
DB=USPT; PLUR=YES; OP=ADJ			
L9	L8 not l3	1	L9
L8	L6 not l2	30	L8

L7	L6 not l2 not l3 not l4	0	L7
L6	L5 not l2-l4	38	L6
L5	l1 and retinal	38	L5
L4	l1 and (voice or print or imprint or eye$ or scan or fingerprint) not l3 not l2	118	L4
L3	l1 and biometric not l2	38	L3
L2	l1 same biometric	8	L2
L1	((without near5 card) near5 transaction)	243	L1

END OF SEARCH HISTORY

WEST Search History

DATE: Monday, October 27, 2003

Set Name side by side	Query	Hit Count	Set Name result set
DB=USPT,PGPB,JPAB,EPAB,DWPI,TDBD; PLUR=YES; OP=ADJ			
L38	L19 not @ad>1995 and transaction	3	L38
L37	L19 not @py>1995 and transaction	30	L37
L36	L35 and transaction	189	L36
L35	L19 not @py<1995	539	L35
L34	L19 same transaction	47	L34
L33	L30 and L19 same transaction	0	L33
L32	L30 and transaction	0	L32
L31	L30 same transaction	0	L31
L30	L29 not l24	534	L30
L29	L19 not @ad<1984	747	L29
L28	l19 and @ad>=1984 and transaction	210	L28
L27	l19 not @ad>=1984 and transaction	3	L27
L26	l19 not @ad>=1984 same transaction	747	L26
L25	l19 not @ad<=1984 same transaction	747	L25
L24	l19 not @ad<=1984 and transaction	213	L24
L23	l22 and transaction	8	L23
L22	L19 not @py>1984	66	L22
L21	L20 not @py>1984	7	L21
L20	L19 and 1984	36	L20
L19	without near5 $card same (voice or print or imprint or eye$ or scan or fingerprint or iris or retinal or biometric) not l1 not l18 not l17	747	L19
DB=USPT; PLUR=YES; OP=ADJ			
L18	((without near5 $card) with transaction) same (voice or print or imprint or eye$ or scan or fingerprint or iris or retinal) not l1	3	L18
DB=USPT,PGPB,JPAB,EPAB,DWPI,TDBD; PLUR=YES; OP=ADJ			
L17	((without near5 card) with transaction) same (voice or print or imprint or eye$ or scan or fingerprint or iris or retinal) not l1	26	L17
DB=USPT; PLUR=YES; OP=ADJ			
L16	((without near5 card) with transaction) same (voice or print or imprint or eye$ or scan or fingerprint or iris or retinal) not l1	3	L16
DB=JPAB,EPAB,DWPI,TDBD; PLUR=YES; OP=ADJ			
L15	((without near5 card) near5 transaction) same biometric	1	L15

DB=USPT; PLUR=YES; OP=ADJ

L14	L13 not l5	88	L14
L13	L12 not l8	88	L13
L12	L11 not l6	88	L12
L11	l1 not l4	125	L11

DB=USPT,PGPB; PLUR=YES; OP=ADJ

L10	cardless near5 transaction	20	L10

DB=USPT; PLUR=YES; OP=ADJ

L9	L8 not l3	1	L9
L8	L6 not l2	30	L8
L7	L6 not l2 not l3 not l4	0	L7
L6	L5 not l2-l4	38	L6
L5	l1 and retinal	38	L5
L4	l1 and (voice or print or imprint or eye$ or scan or fingerprint) not l3 not l2	118	L4
L3	l1 and biometric not l2	38	L3
L2	l1 same biometric	8	L2
L1	((without near5 card) near5 transaction)	243	L1

END OF SEARCH HISTORY

WEST Search History

DATE: Monday, October 27, 2003

Set Name side by side	Query	Hit Count	Set Name result set
DB=USPT,PGPB,JPAB,EPAB,DWPI,TDBD; PLUR=YES; OP=ADJ			
L4	author$ without $card same (biometric$ or iris or scan or retinal or fingerprint or print or imprint or eye)	0	L4
DB=USPT; PLUR=YES; OP=ADJ			
L3	author$ without $card same (biometric$ or iris or scan or retinal or fingerprint or print or imprint or eye)	0	L3
L2	author$ without $card same (biometric$ or iris or scan or retinal or fingerprint or print oo imprint or eye)	0	L2
L1	author$ without card same (biometric$ or iris or scan or retinal or fingerprint or print oo imprint or eye)	0	L1

END OF SEARCH HISTORY

```
B EECOMP
       27oct03 15:55:40 User268094 Session D26.1
            $0.00    0.230 DialUnits FileHomeBase
     $0.00  Estimated cost FileHomeBase
     $0.46  INTERNET
     $0.46  Estimated cost this search
     $0.46  Estimated total session cost   0.230 DialUnits

SYSTEM:OS  - DIALOG OneSearch
  File   2:INSPEC  1969-2003/Oct W3
         (c) 2003 Institution of Electrical Engineers
 *File   2: Alert feature enhanced for multiple files, duplicates
removal, customized scheduling. See HELP ALERT.
  File   6:NTIS  1964-2003/Oct W4
         (c) 2003 NTIS, Intl Cpyrght All Rights Res
  File   8:Ei Compendex(R)  1970-2003/Oct W3
         (c) 2003 Elsevier Eng.  Info. Inc.
  File  25:Weldasearch  1966-2002/Apr
         (c) 2003 TWI Ltd
  File  34:SciSearch(R) Cited Ref Sci  1990-2003/Oct W3
         (c) 2003 Inst for Sci Info
  File  65:Inside Conferences  1993-2003/Oct W4
         (c) 2003 BLDSC all rts. reserv.
  File  92:IHS Intl.Stds.& Specs.  1999/Nov
         (c) 1999 Information Handling Services
 *File 92: This file is closed (no updates)
  File  94:JICST-EPlus  1985-2003/Oct W4
         (c)2003 Japan Science and Tech Corp(JST)
  File  95:TEME-Technology & Management  1989-2003/Oct W1
         (c) 2003 FIZ TECHNIK
  File  99:Wilson Appl. Sci & Tech Abs  1983-2003/Sep
         (c) 2003 The HW Wilson Co.
  File 103:Energy SciTec  1974-2003/Oct B1
         (c) 2003 Contains copyrighted material
 *File 103: For access restrictions see Help Restrict.
  File 144:Pascal  1973-2003/Oct W3
         (c) 2003 INIST/CNRS
  File 239:Mathsci  1940-2003/Dec
         (c) 2003 American Mathematical Society
  File 241:Elec. Power DB  1972-1999Jan
         (c) 1999 Electric Power Research Inst.Inc
 *File 241: This file is closed (no updates)
  File 434:SciSearch(R) Cited Ref Sci  1974-1989/Dec
         (c) 1998 Inst for Sci Info
  File 647:CMP  Computer Fulltext  1988-2003/Sep W3
         (c) 2003 CMP Media, LLC

      Set  Items  Description
      ---  -----  -----------
?
```

```
S AUTHOR$ (5N) WITHOUT (5N) $CARD (5N) (BIOMETRIC$ OR IRIS OR SCAN OR RE
                0  AUTHOR$
          1982586  WITHOUT
                0  $CARD
                0  BIOMETRIC$
            27320  IRIS
           172843  SCAN
           123688  RETINAL
            17853  FINGERPRINT
            47786  PRINT
             6510  IMPRINT
           411583  EYE
       S1       0  AUTHOR$ (5N) WITHOUT (5N) $CARD (5N) (BIOMETRIC$ OR IR
                   OR SCAN OR RETINAL OR FINGERPRINT OR PRINT OR IMPRINT
                   EYE)
?
```

```
S AUTHOR$ (5N) WITHOUT (5N) CARD (5N) (BIOMETRIC$ OR IRIS OR SCAN OR RET
                0  AUTHOR$
          1982586  WITHOUT
            87302  CARD
                0  BIOMETRIC$
            27320  IRIS
           172843  SCAN
           123688  RETINAL
            17853  FINGERPRINT
            47786  PRINT
             6510  IMPRINT
           411583  EYE
       S2        0  AUTHOR$ (5N) WITHOUT (5N) CARD (5N) (BIOMETRIC$ OR IRI
                    OR SCAN OR RETINAL OR FINGERPRINT OR PRINT OR IMPRINT
                    EYE)
?
```

```
S AUTHOR$ (5N) WITHOUT (5N) CARD (5N) (BIOMETRIC$ OR IRIS OR SCAN OR RET
                0  AUTHOR$
          1982586  WITHOUT
            87302  CARD
                0  BIOMETRIC$
            27320  IRIS
           172843  SCAN
           123688  RETINAL
            17853  FINGERPRINT
            47786  PRINT
             6510  IMPRINT
           411583  EYE
       S2       0  AUTHOR$ (5N) WITHOUT (5N) CARD (5N) (BIOMETRIC$ OR IRI
                   OR SCAN OR RETINAL OR FINGERPRINT OR PRINT OR IMPRINT
                   EYE)
?
```

```
S AUTHOR? (5N) WITHOUT (5N) CARD (5N) (BIOMETRIC? OR IRIS OR SCAN OR RET
         7332958  AUTHOR?
         1982586  WITHOUT
           87302  CARD
           16675  BIOMETRIC?
           27320  IRIS
          172843  SCAN
          123688  RETINAL
           17853  FINGERPRINT
           47786  PRINT
            6510  IMPRINT
          411583  EYE
      S4       0  AUTHOR? (5N) WITHOUT (5N) CARD (5N) (BIOMETRIC? OR IRI
                  OR SCAN OR RETINAL OR FINGERPRINT OR PRINT OR IMPRINT
                  EYE)
?
```

```
S TRANSACTION (5N) WITHOUT (5N) CARD (5N) (BIOMETRIC? OR IRIS OR SCAN OR
           47495  TRANSACTION
         1982586  WITHOUT
           87302  CARD
           16675  BIOMETRIC?
           27320  IRIS
          172843  SCAN
          123688  RETINAL
           17853  FINGERPRINT
           47786  PRINT
            6510  IMPRINT
          411583  EYE
      S5       0  TRANSACTION (5N) WITHOUT (5N) CARD (5N) (BIOMETRIC? OR
                  IRIS OR SCAN OR RETINAL OR FINGERPRINT OR PRINT OR
                  IMPRINT OR EYE)
?
```

```
S TRANSACTION (W) WITHOUT (W) CARD (W) (BIOMETRIC? OR IRIS OR SCAN OR RE
          47495  TRANSACTION
        1982586  WITHOUT
          87302  CARD
          16675  BIOMETRIC?
          27320  IRIS
         172843  SCAN
         123688  RETINAL
          17853  FINGERPRINT
          47786  PRINT
           6510  IMPRINT
         411583  EYE
      S6      0  TRANSACTION (W) WITHOUT (W) CARD (W) (BIOMETRIC? OR IF
                 OR SCAN OR RETINAL OR FINGERPRINT OR PRINT OR IMPRINT
                 EYE)
?
```

```
B ELECTRON
       27oct03 16:03:14 User268094 Session D26.2
            $2.11    0.295 DialUnits File2
     $2.11  Estimated cost File2
            $0.91    0.154 DialUnits File6
     $0.91  Estimated cost File6
            $2.27    0.325 DialUnits File8
     $2.27  Estimated cost File8
            $0.21    0.059 DialUnits File25
     $0.21  Estimated cost File25
            $3.91    0.212 DialUnits File34
     $3.91  Estimated cost File34
            $0.30    0.081 DialUnits File65
     $0.30  Estimated cost File65
            $0.18    0.056 DialUnits File92
     $0.18  Estimated cost File92
            $0.82    0.235 DialUnits File94
     $0.82  Estimated cost File94
            $0.67    0.096 DialUnits File95
     $0.67  Estimated cost File95
            $0.20    0.084 DialUnits File99
     $0.20  Estimated cost File99
            $0.85    0.168 DialUnits File103
     $0.85  Estimated cost File103
            $0.62    0.178 DialUnits File144
     $0.62  Estimated cost File144
            $0.85    0.212 DialUnits File239
     $0.85  Estimated cost File239
            $0.21    0.051 DialUnits File241
     $0.21  Estimated cost File241
            $1.28    0.069 DialUnits File434
     $1.28  Estimated cost File434
            $0.53    0.103 DialUnits File647
     $0.53  Estimated cost File647
            OneSearch, 16 files,  2.376 DialUnits FileOS
     $1.86  INTERNET
    $17.78  Estimated cost this search
    $18.24  Estimated total session cost   2.606 DialUnits

SYSTEM:OS  - DIALOG OneSearch
  File   9:Business & Industry(R)  Jul/1994-2003/Oct 24
         (c) 2003 Resp. DB Svcs.
  File  15:ABI/Inform(R)  1971-2003/Oct 25
         (c) 2003 ProQuest Info&Learning
 *File  15: Alert feature enhanced for multiple files, duplicate
removal, customized scheduling. See HELP ALERT.
  File  16:Gale Group PROMT(R)  1990-2003/Oct 24
         (c) 2003 The Gale Group
 *File  16: Alert feature enhanced for multiple files, duplicate
removal, customized scheduling. See HELP ALERT.
  File  18:Gale Group F&S Index(R)  1988-2003/Oct 27
         (c) 2003 The Gale Group
  File  20:Dialog Global Reporter  1997-2003/Oct 27
         (c) 2003 The Dialog Corp.
```

```
  File  80:TGG Aerospace/Def.Mkts(R)  1986-2003/Oct 24
        (c) 2003 The Gale Group
  File 148:Gale Group Trade & Industry DB  1976-2003/Oct 27
        (c)2003 The Gale Group
 *File 148: Alert feature enhanced for multiple files, duplicate
removal, customized scheduling. See HELP ALERT.
  File 160:Gale Group PROMT(R)  1972-1989
        (c) 1999 The Gale Group
  File 256:SoftBase:Reviews,Companies&Prods.  82-2003/Sep
        (c)2003 Info.Sources Inc
  File 275:Gale Group Computer DB(TM)  1983-2003/Oct 24
        (c) 2003 The Gale Group
  File 481:DELPHES Eur Bus  95-2003/Oct W3
        (c) 2003 ACFCI & Chambre CommInd Paris
  File 583:Gale Group Globalbase(TM)  1986-2002/Dec 13
        (c) 2002 The Gale Group
 *File 583: This file is no longer updating as of 12-13-2002.
  File 621:Gale Group New Prod.Annou.(R)  1985-2003/Oct 27
        (c) 2003 The Gale Group
  File 624:McGraw-Hill Publications  1985-2003/Oct 27
        (c) 2003 McGraw-Hill Co. Inc
 *File 624: Homeland Security & Defense and 9 Platt energy journals adde
Please see HELP NEWS624 for more
  File 635:Business Dateline(R)  1985-2003/Oct 25
        (c) 2003 ProQuest Info&Learning
  File 636:Gale Group Newsletter DB(TM)  1987-2003/Oct 24
        (c) 2003 The Gale Group
  File 647:CMP  Computer Fulltext  1988-2003/Sep W3
        (c) 2003 CMP Media, LLC
  File 674:Computer News Fulltext  1989-2003/Oct W4
        (c) 2003 IDG Communications
  File 696:DIALOG Telecom. Newsletters  1995-2003/Oct 25
        (c) 2003 The Dialog Corp.

      Set  Items  Description
      ---  -----  -----------
?
```

```
S TRANSACTION (W) WITHOUT (W) CARD (W) (BIOMETRIC? OR IRIS OR SCAN OR RE
Processed  10 of  19 files ...
Processing
Completed processing all files
         1870736  TRANSACTION
         6751409  WITHOUT
         1740181  CARD
           49468  BIOMETRIC?
           53761  IRIS
          242616  SCAN
           13325  RETINAL
           39941  FINGERPRINT
         1122915  PRINT
           44795  IMPRINT
          957546  EYE
      S1       0  TRANSACTION (W) WITHOUT (W) CARD (W) (BIOMETRIC? OR IF
                  OR SCAN OR RETINAL OR FINGERPRINT OR PRINT OR IMPRINT
                  EYE)
?
```

```
B BUSECON
       27oct03 16:04:26 User268094 Session D26.3
            $0.29    0.054 DialUnits File9
     $0.29  Estimated cost File9
            $0.42    0.078 DialUnits File15
     $0.42  Estimated cost File15
            $0.59    0.110 DialUnits File16
     $0.59  Estimated cost File16
            $0.11    0.024 DialUnits File18
     $0.11  Estimated cost File18
            $0.21    0.215 DialUnits File20
     $0.21  Estimated cost File20
            $0.08    0.015 DialUnits File80
     $0.08  Estimated cost File80
            $0.59    0.110 DialUnits File148
     $0.59  Estimated cost File148
            $0.12    0.021 DialUnits File160
     $0.12  Estimated cost File160
            $0.08    0.015 DialUnits File256
     $0.08  Estimated cost File256
            $0.27    0.050 DialUnits File275
     $0.27  Estimated cost File275
            $0.05    0.013 DialUnits File481
     $0.05  Estimated cost File481
            $0.10    0.030 DialUnits File583
     $0.10  Estimated cost File583
            $0.31    0.058 DialUnits File621
     $0.31  Estimated cost File621
            $0.18    0.032 DialUnits File624
     $0.18  Estimated cost File624
            $0.27    0.050 DialUnits File635
     $0.27  Estimated cost File635
            $0.34    0.063 DialUnits File636
     $0.34  Estimated cost File636
            $0.08    0.015 DialUnits File647
     $0.08  Estimated cost File647
            $0.09    0.021 DialUnits File674
     $0.09  Estimated cost File674
            $0.19    0.034 DialUnits File696
     $0.19  Estimated cost File696
            OneSearch, 19 files,  1.006 DialUnits FileOS
     $0.46  INTERNET
     $4.83  Estimated cost this search
    $23.07  Estimated total session cost   3.612 DialUnits

SYSTEM:OS  - DIALOG OneSearch
  File   9:Business & Industry(R)  Jul/1994-2003/Oct 24
         (c) 2003 Resp. DB Svcs.
  File  13:BAMP  2003/Oct W3
         (c) 2003 Resp. DB Svcs.
  File  15:ABI/Inform(R)  1971-2003/Oct 25
         (c) 2003 ProQuest Info&Learning
 *File  15: Alert feature enhanced for multiple files, duplicate
removal, customized scheduling. See HELP ALERT.
```

File 16:Gale Group PROMT(R) 1990-2003/Oct 24
(c) 2003 The Gale Group
***File 16: Alert feature enhanced for multiple files, duplicate removal, customized scheduling. See HELP ALERT.**
File 20:Dialog Global Reporter 1997-2003/Oct 27
(c) 2003 The Dialog Corp.
File 30:AsiaPacific 1985-2003/Oct 27
(c) 2003 Aristarchus Knowledge Indus.
File 75:TGG Management Contents(R) 86-2003/Oct W2
(c) 2003 The Gale Group
File 93:TableBase(R) Sep 1997-2003/Oct W3
(c) 2003 Resp. DB Svcs.
File 111:TGG Natl.Newspaper Index(SM) 1979-2003/Oct 22
(c) 2003 The Gale Group
File 139:EconLit 1969-2003/Oct
(c) 2003 American Economic Association
File 148:Gale Group Trade & Industry DB 1976-2003/Oct 27
(c)2003 The Gale Group
***File 148: Alert feature enhanced for multiple files, duplicate removal, customized scheduling. See HELP ALERT.**
File 160:Gale Group PROMT(R) 1972-1989
(c) 1999 The Gale Group
File 211:Gale Group Newsearch(TM) 2003/Oct 27
(c) 2003 The Gale Group
File 249:PIRA Mgt. & Mktg. Abs. 1976-2003Oct W3
(c) 2003 Pira International
File 466:Info Latino America 1988-1995/Dec W1
(c) 1997 Info-South
***File 466: This is a closed file.**
File 476:Financial Times Fulltext 1982-2003/Oct 27
(c) 2003 Financial Times Ltd
File 481:DELPHES Eur Bus 95-2003/Oct W3
(c) 2003 ACFCI & Chambre CommInd Paris
File 484:Periodical Abs Plustext 1986-2003/Oct W3
(c) 2003 ProQuest
***File 484: SELECT IMAGE AVAILABILITY FOR PROQUEST FILES**
ENTER 'HELP PROQUEST' FOR MORE
File 485:Accounting & Tax DB 1971-2003/Oct W3
(c) 2003 ProQuest Info&Learning
***File 485: SELECT IMAGE AVAILABILITY FOR PROQUEST FILES**
ENTER 'HELP PROQUEST' FOR MORE
File 553:Wilson Bus. Abs. FullText 1982-2003/Sep
(c) 2003 The HW Wilson Co
File 583:Gale Group Globalbase(TM) 1986-2002/Dec 13
(c) 2002 The Gale Group
***File 583: This file is no longer updating as of 12-13-2002.**
File 620:EIU:Viewswire 2003/Oct 24
(c) 2003 Economist Intelligence Unit
File 622:EIU Magazines 2000-2003/Oct 28
(c) 2003 EIU Magazines
File 624:McGraw-Hill Publications 1985-2003/Oct 27
(c) 2003 McGraw-Hill Co. Inc
***File 624: Homeland Security & Defense and 9 Platt energy journals adde**

```
Please see HELP NEWS624 for more
  File 627:EIU: Country Analysis  2003/Oct W3
         (c) 2003 Economist Intelligence Unit
  File 628:Ctry Risk & Forecasts  2003/Oct W3
         (c) 2003 Economist Intelligence Unit
 *File 628: Prices are changing Nov. 1.  Please see HELP NEWS628.
  File 629:EIU:BUS. Newsletters  2003/Oct W3
         (c) 2003 Economist Intelligence Unit
 *File 629: Prices are changing Nov. 1.  Please see HELP NEWS629.
  File 636:Gale Group Newsletter DB(TM)  1987-2003/Oct 24
         (c) 2003 The Gale Group
  File 637:Journal of Commerce  1986-2003/Oct 29
         (c) 2003 Commonwealth Bus. Media

      Set  Items  Description
      ---  -----  -----------
?
```

```
S TRANSACTION (W) WITHOUT (W) CARD (W) (BIOMETRIC? OR IRIS OR SCAN OR RE
Processed  20 of  29 files ...
Processing
Completed processing all files
         1694737  TRANSACTION
         7015397  WITHOUT
         1593581  CARD
           45736  BIOMETRIC?
           54167  IRIS
          212498  SCAN
           14298  RETINAL
           37310  FINGERPRINT
         1063080  PRINT
           51044  IMPRINT
         1037282  EYE
      S1       0  TRANSACTION (W) WITHOUT (W) CARD (W) (BIOMETRIC? OR IF
                  OR SCAN OR RETINAL OR FINGERPRINT OR PRINT OR IMPRINT
                  EYE)
?
```

```
B COMPSCI
      27oct03 16:05:34 User268094 Session D26.4
            $0.18    0.033 DialUnits File9
      $0.18 Estimated cost File9
            $0.20    0.037 DialUnits File13
      $0.20 Estimated cost File13
            $0.24    0.045 DialUnits File15
      $0.24 Estimated cost File15
            $0.48    0.089 DialUnits File16
      $0.48 Estimated cost File16
            $0.19    0.186 DialUnits File20
      $0.19 Estimated cost File20
            $0.01    0.015 DialUnits File30
      $0.01 Estimated cost File30
            $0.11    0.024 DialUnits File75
      $0.11 Estimated cost File75
            $0.12    0.017 DialUnits File93
      $0.12 Estimated cost File93
            $0.10    0.029 DialUnits File111
      $0.10 Estimated cost File111
            $0.07    0.021 DialUnits File139
      $0.07 Estimated cost File139
            $0.50    0.093 DialUnits File148
      $0.50 Estimated cost File148
            $0.09    0.016 DialUnits File160
      $0.09 Estimated cost File160
            $0.07    0.016 DialUnits File211
      $0.07 Estimated cost File211
            $0.07    0.012 DialUnits File249
      $0.07 Estimated cost File249
            $0.02    0.016 DialUnits File466
      $0.02 Estimated cost File466
            $0.03    0.029 DialUnits File476
      $0.03 Estimated cost File476
            $0.02    0.007 DialUnits File481
      $0.02 Estimated cost File481
            $0.25    0.051 DialUnits File484
      $0.25 Estimated cost File484
            $0.21    0.035 DialUnits File485
      $0.21 Estimated cost File485
            $0.07    0.029 DialUnits File553
      $0.07 Estimated cost File553
            $0.05    0.015 DialUnits File583
      $0.05 Estimated cost File583
            $0.07    0.019 DialUnits File620
      $0.07 Estimated cost File620
            $0.07    0.017 DialUnits File622
      $0.07 Estimated cost File622
            $0.10    0.017 DialUnits File624
      $0.10 Estimated cost File624
            $0.13    0.021 DialUnits File627
      $0.13 Estimated cost File627
            $0.10    0.016 DialUnits File628
      $0.10 Estimated cost File628
```

```
            $0.08    0.019 DialUnits File629
      $0.08 Estimated cost File629
            $0.22    0.040 DialUnits File636
      $0.22 Estimated cost File636
            $0.10    0.020 DialUnits File637
      $0.10 Estimated cost File637
            OneSearch, 29 files,  0.984 DialUnits FileOS
      $0.46 INTERNET
      $4.41 Estimated cost this search
     $27.48 Estimated total session cost   4.596 DialUnits

SYSTEM:OS  - DIALOG OneSearch
  File   2:INSPEC  1969-2003/Oct W3
         (c) 2003 Institution of Electrical Engineers
 *File   2: Alert feature enhanced for multiple files, duplicates
removal, customized scheduling. See HELP ALERT.
  File   6:NTIS  1964-2003/Oct W4
         (c) 2003 NTIS, Intl Cpyrght All Rights Res
  File   8:Ei Compendex(R)  1970-2003/Oct W3
         (c) 2003 Elsevier Eng.  Info. Inc.
  File  34:SciSearch(R) Cited Ref Sci  1990-2003/Oct W3
         (c) 2003 Inst for Sci Info
  File  35:Dissertation Abs Online  1861-2003/Sep
         (c) 2003 ProQuest Info&Learning
  File  65:Inside Conferences  1993-2003/Oct W4
         (c) 2003 BLDSC all rts. reserv.
  File  92:IHS Intl.Stds.& Specs.  1999/Nov
         (c) 1999 Information Handling Services
 *File 92: This file is closed (no updates)
  File  94:JICST-EPlus  1985-2003/Oct W4
         (c)2003 Japan Science and Tech Corp(JST)
  File  95:TEME-Technology & Management  1989-2003/Oct W1
         (c) 2003 FIZ TECHNIK
  File  99:Wilson Appl. Sci & Tech Abs  1983-2003/Sep
         (c) 2003 The HW Wilson Co.
  File 103:Energy SciTec  1974-2003/Oct B1
         (c) 2003 Contains copyrighted material
 *File 103: For access restrictions see Help Restrict.
  File 144:Pascal  1973-2003/Oct W3
         (c) 2003 INIST/CNRS
  File 202:Info. Sci. & Tech. Abs.  1966-2003/Sep 16
         (c) 2003 EBSCO Publishing
  File 233:Internet & Personal Comp. Abs.  1981-2003/Jul
         (c) 2003, EBSCO Pub.
  File 239:Mathsci  1940-2003/Dec
         (c) 2003 American Mathematical Society
  File 275:Gale Group Computer DB(TM)  1983-2003/Oct 24
         (c) 2003 The Gale Group
  File 434:SciSearch(R) Cited Ref Sci  1974-1989/Dec
         (c) 1998 Inst for Sci Info
  File 647:CMP  Computer Fulltext  1988-2003/Sep W3
         (c) 2003 CMP Media, LLC
  File 674:Computer News Fulltext  1989-2003/Oct W4
```

File 696:DIALOG Telecom. Newsletters 1995-2003/Oct 25

Set	Items	Description

?

```
S TRANSACTION AND WITHOUT AND CARD AND (BIOMETRIC? OR IRIS OR SCAN OR RE
          110950  TRANSACTION
         2294672  WITHOUT
          234522  CARD
           19975  BIOMETRIC?
           30808  IRIS
          201829  SCAN
          126357  RETINAL
           20698  FINGERPRINT
          136028  PRINT
            7540  IMPRINT
          446921  EYE
      S2    1138  TRANSACTION AND WITHOUT AND CARD AND (BIOMETRIC? OR IF
                  OR SCAN OR RETINAL OR FINGERPRINT OR PRINT OR IMPRINT
                  EYE)
?
```

```
S TRANSACTION (W) WITHOUT (W) CARD AND (BIOMETRIC? OR IRIS OR SCAN OR RE
          110950  TRANSACTION
         2294672  WITHOUT
          234522  CARD
               0  TRANSACTION(W)WITHOUT(W)CARD
           19975  BIOMETRIC?
           30808  IRIS
          201829  SCAN
          126357  RETINAL
           20698  FINGERPRINT
          136028  PRINT
            7540  IMPRINT
          446921  EYE
      S3        0  TRANSACTION (W) WITHOUT (W) CARD AND (BIOMETRIC? OR IF
                   OR SCAN OR RETINAL OR FINGERPRINT OR PRINT OR IMPRINT
                   EYE)
?
```

ProQuest® Help

Basic Search | Topic Guide | Publication Search | Marked List | Interface language: English

Databases selected: Multiple databases...

Results

- **9** articles found for: *(transaction) AND (card) AND (biometric) AND PDN(<12/29/1994)*

All sources | Scholarly Journals | Magazines | Trade Publications | Newspapers

Mark / Clear all on page | View marked articles | Full text articles only | Sort results by: Most recent articles first

1. **Life at the International Bank of Canada**
d Aoust, Janyne. **Canadian Banker (Online).** Toronto: Nov/Dec 1993. Vol. 100, Iss. 6; p. 31 (1 page)
Full text | Abstract

2. **Diversity in the District**
Harowitz, Sherry L. **Security Management.** Arlington: Sep 1993. Vol. 37, Iss. 9; p. 48 (8 pages)
Full text | Abstract

3. **Automated fingerprint analysis offers fast verification**
Hollingum, Jack. **Sensor Review.** Bradford: 1992. Vol. 12, Iss. 3; p. 12 (4 pages)
Full text | Abstract

4. **Biometrics - When the person is the key**
Jennings, Chris. **Sensor Review.** Bradford: 1992. Vol. 12, Iss. 3; p. 9 (3 pages)
Full text | Abstract

5. **Data Security: The Best Insurance**
Ronne, George E.. **Best's Review (Property/casualty insurance edition).** Oldwick: Apr 1991. Vol. 91, Iss. 12; p. 74 (3 pages)
Full text | Page Image - PDF | Abstract

6. **Data Security: The Best Insurance**
Ronne, George E.. **Best's Review (Life/health insurance edition).** Oldwick: Apr 1991. Vol. 91, Iss. 12; p. 72 (4 pages)
Full text | Page Image - PDF | Abstract

7. **Identix in Multinational Program to Produce Smart Card/Biometric Transaction Terminal**
Hawks, Randy, Schuster, Ray. **Business Wire.** New York: Jun 15, 1990. p. 1
Full text | Abstract

8. **Fingerprint Technology Makes for Best ID System**
Rechtin, Mark. **Orange County Business Journal.** Newport Beach: May 14, 1990. Vol. 12, Iss. 51; p. 7
Full text | Abstract

9. **A Comeback for the Signature? Technology Vendors Renewing Efforts on Electronic Verification**

Biometrics - When the person is the key

Jennings, Chris. **Sensor Review**. Bradford: 1992. Vol. 12, Iss. 3; pg. 9, 3 pgs

Subjects:	Voice recognition, Security systems, Product development, Product design, Electronics industry, Effectiveness, Case studies, Biometrics
Classification Codes	9175, 9110, 8650, 7500, 5240, 5140
Locations:	UK
Companies:	Zetetic International PLC
Author(s):	Jennings, Chris
Publication title:	Sensor Review. Bradford: 1992. Vol. 12, Iss. 3; pg. 9, 3 pgs
Source Type:	Periodical
ISSN/ISBN:	02602288
ProQuest document ID:	1310034
Text Word Count	2098
Article URL:	http://gateway.proquest.com/openurl?ctx_ver=z39.88-2003&res_id=xri:pqd&rft_val_fmt=ori:fmt:kev:mtx:journal&genre=article&rft_id=xri:pqd:did=000000001310034&svc_dat=xri:pqil:fmt=text&req_dat=xri:pqil:pq_clntid=19649

Abstract (Article Summary)

Unlike the typical security system, where there is no certainty that the rightful owner has used it, biometric security devices operate by detecting a physically different characteristic that is unique to an individual. Zetetic International of Nottingham, UK, has a patented approach to using voice as a biometric system. The Zi2000 Voice Recognition System (VRS) is based on the fact that different sounds in any language are largely made by different physical parts of the vocal tract. The Zi2000 VRS uses 5 different sound types and has a special 250-word vocabulary for each language. To enroll a person onto the system, the user is randomly presented by the computer with 3 different words for each group. These 15 words are repeated 5 times to produce a template of each word. To use the system, the user informs the Zi2000 VRS who is purporting to enter. The Zi2000 VRS then randomly picks out of the 15-word vocabulary 5 words for the user to repeat. When the user has spoken them into a free-standing microphone or a handset and the computer has compared them with the stored templates, access is then granted. The accuracy of the system, because it uses 5 different physical characteristics, is very high. The false acceptance rate is calculated at about one in 10 million.

Full Text (2098 words)

From the earliest time, guards have been used to control access to certain areas. Guards are people and, however conscientious, they are forgetful, bribable, coercible or just plain inefficient. The introduction of the key and lock provided the first automated assistance to control access and, despite the ingenuity of locksmiths, keys can be stolen, duplicated or lost and locks can be picked.

Today's "state-of-the-art" traditional access control techniques are unfortunately just like the key and lock system. Passwords, PIN numbers, magnetic stripe cards, Smart cards and the rest have to be remembered to be carried around and have to be kept secure. We all know of the inconvenience of mislaying a key or the frisson of fear when a credit card is not where it ought to be. Whatever the system, the only known thing is that if the correct card, key, PIN number, etc. has been used, there is no certainty that the rightful owner has used it.

BIOMETRIC SYSTEMS

Biometric devices work on the detection of a physically different characteristic which is unique to an individual. Over

the years many different ones have been tried, e.g. weight, finger length, palm prints, eye retina, keyboard rhythms, hand shapes, fingerprints, signature action, voice and others. Basically, in all biometric systems, the characteristic has to be measured and then the reading has to be compared with a previously stored reading. This comparison score is a measure of how close the new reading is to the stored reading. Below a certain predetermined threshold, the new reading is deemed to be a match.

The measurement device, in a biometric system for normal use as an access control system, has to be rugged and fast and of course cannot be as accurate as that achievable in a laboratory environment. However, most measurement devices are over 98 per cent accurate, though some are more expensive than others, e.g. scanners for fingerprints versus a microphone and analogue-to-digital converter for voice. The accuracy of measuring only one biometric feature (with, for example, a 2 per cent error) is still dramatically better in checking that the rightful user has gained entry than any non-biometric system. However, it could cause problems for rightful users if they are rejected by the system. False acceptance (where B is accepted as if they were A) and false rejection (where A is rejected even though A is permitted entry) are two measures of a biometric system. They are related to each other and in general if one is improved, the other deteriorates.

Different applications need different combinations. For example, a bank vault access control system needs to have zero false accepts whereas a credit card control system needs to have zero false rejects. The bank vault application can tolerate a few false rejects and the credit card system can tolerate a few false accepts. In all cases a good biometric system is inherently an order of magnitude more secure than any non-biometric system.

Measuring more than one biometric feature (e.g. several different fingerprints, several different sound types) again dramatically improves the security of a biometric system. For example:

(1) For a one-biometric system, measured with 99 per cent accuracy, the system is wrong approximately once in every 100 times it is used.

(2) For a two-biometric system, measured with 99 per cent accuracy for each feature, the system is wrong approximately only once every 10,000 times.

Some biometric features do not change significantly with time, e.g. hand shapes and eye retinas. Others are different every time they are measured, e.g. signature action and the voice. These latter "active" biometric features cannot be artificially modelled to trick a system and thus provide an extra layer of security in use.

As biometric systems are new to the marketplace, users are still familiarizing themselves with these new machines. However, it is already clear that people are happy to use a signature or utter a few words as the means of entering or authorizing.

Thus a good biometric system, to solve a particular access control problem, has to measure more than one biometric feature, balance the false accepts and false rejects, be user friendly and of course be competitive on price, performance and speed of use.

Biometric devices are available on the market to perform the following functions:

* access control for networks of doors in a building

* access control for networks of doors with different levels of security risk

* access control for safes, automatic teller machines (bank side)

* children's pick-up at day care centres

* access control for specific rooms, laboratories, computer rooms, etc.

* passport control--frequent users

* control of access to computers, computer networks, applications programs, files and transactions

* on-line/off-line credit card authorization at point of sale.

In the near term, biometric devices will be available for normal home use (front and back door), locking systems for motor vehicles, authorization of credit calls over the telephone network, authorization of central control intruder

alarm systems, etc.

At the moment, biometric devices installed for access control are small in number compared to magnetic stripe card systems. However, the cost of manufacture is set to drop, dramatically as the volumes of production increase. Biometric access control systems will be rivalling the stripe card on a price-per-door basis in the next I2 months. Home access control systems could be on the market for about L150 within a year as well.

VOICE RECOGNITION SYSTEMS

Zetetic International of Nottingham have a patented approach to using voice as a biometric system. Their Zi2000 Voice Recognition System won the Prince of Wales Award for Innovation in 1992 and has become "the product of the year", an award from the Canadian Security Association.

The Zi2000 VRS approach is based on the fact that different sounds in any language are largely made by different physical parts of the vocal tract. For example, the "p" in the English word "pack" is made by the lips, and the "t" in "tack" is made by the tip of the tongue. The "ck" in both cases is made by the back of the tongue hitting the back of the throat. Much the same as the fact that external features, a nose, are different between people so is the shape of the vocal tract.

The Zi2000 VRS System uses five different sound types and has a special 250-word vocabulary for each language. Users are recommended to speak in their native tongue, as this ensures good consistency in their pronunciation of words. The 250-word vocabulary is divided into groups of 50 words, each containing one of the five different sound types.

To enrol a person onto the system, the user is randomly presented by the computer with three different words from each group. These 15 words are repeated five times, to produce a template of each word. This process takes about two-and-a-half minutes. The users have the option of choosing another word if they are not happy with the word presented.

To use the system, the user informs the Zi2000 VRS who is purporting to enter. This is done by keying in the user name (in a computer network security application) or entering a non-secret PIN, using a proximity card or even speaking the name (for an access control system). The Zi2000 VRS then randomly picks out of the 15-word vocabulary five words for the user to repeat. These are displayed on a screen. When the user has spoken them into a free-standing microphone (access control system) or a handset (computer applications), and the computer has compared them with the stored templates, access is then granted. This takes about ten seconds. The user is allowed up to five attempts for each word. This is in case of stammering or extraneous noise like a door slamming.

As human voices vary over time (several months for males, and monthly for females; and it also varies depending on the ambient temperature) each successful use of the system causes the original templates to be slightly modified. This improves the false reject statistics.

The control of the Zi2000 VRS System is in the hands of the security supervisor (normally there are at least two). It can only be placed in enrol mode by the supervisor: having been checked by the usual random five words, the supervisor can then add or delete users. In addition, normal housekeeping (backing up words to tape, etc.) and management functions (downloading entry/exit information) can only be done by the supervisor.

This means that users do not have to keep anything secret, do not need to carry anything on their person, nor do they know what combination of words will appear to obtain access. As the templates are approximately 1,500 bytes in length (uncompressed), the detail of the utterance (the biometric) is impressive. Attempts to record sounds made by a user (apart from probably being obvious to the user), with another microphone do not result in the same 1,500 bytes. This is due to the physical position of the microphone within its casing and the natural standing wave caused by its physical environment.

Eighteen languages, including most European languages, together with Chinese, Japanese and Arabic, are currently available. For each language, the messages used by the Zi2000 VRS System to communicate with the user are in the person's native language. Physically, the Zi2000 VRS ii contained in two units as an access control device (see Figure 1). (Figure 1 omitted)

The access control units are connected on the inside of the protected area to a master unit. This unit contains storage and the computer power to calculate and compare templates. In addition it contains the relays to control door open alarms, electric strikes and other applications. Even with all the covers off, no connections can be made to open a door without proper voice authorization. In a multi-door networked system, all units are connected to a PC

in a secure environment, which maintains the template and full statistics on who is enrolled on the system as well as complete usage data.

For a computer network control system, a VRS card is placed inside the PC with a handset attached. Simple instructions are then inserted in the network control program so that access to the network or application program or even the processing of a transaction can be controlled by the Zi2000 VRS System.

The accuracy of the system, because it uses five different physical characteristics, is very high. The false acceptance rate is calculated at about 1:10 million. The false reject rate is largely a function of the environment of the installation and the acquired habits of the users, and is usually negligible.

Random noises (at the same time as an utterance) will cause the system to reject the utterance, but of course it offers the user another attempt. Normally five utterances (five words, one utterance each) are all that is required but this may be six or seven in some environments.

The system expects users to repeat words consistently with the enrolled utterances. This means that length of utterance, loudness, tone, pronunciation and position relative to the microphone are similar each time This is a learned habit which normally takes a few usages to remember.

Tests have been made with people who were up to double the alcohol limit for driving, and the system still recognized them. Tests on people with colds and sore throats show slightly more utterances required in some circumstances. However, if both nostrils are completely blocked (and cannot be temporarily unblocked), the utterances are largely rejected.

Developments by Zetetic International are ongoing to produce better, cheaper, lower capacity (of users) systems for special applications like home access and car locking systems. In addition, a voice input system is being developed for transaction or order entry direct into a computer. Normal word recognition systems, with training, are still under 100 per cent on recognition of individual words. However, if the user is already authorized by the system, input words such as "10,000" can be recognized every time.

There is no doubt that biometric systems are here to stay. In the near future it looks as though they are going to have an impact on everyone as they start controlling access to doors, computers and authorizing credit card special transactions. People will no longer be able to impersonate others by utilizing their cards or keys. One more worry of modern life will be removed.

Chris Jennings spent 28 years with IBM. He invented the Zi2000 Voice Recognition System and is Managing Director of Zi plc, 8 Faraday Building, Highfields Science Park, University Boulevard, Nottingham NG7 2QP. Tel: 0602 228502; Fax: 0602 225013.

Data Security: The Best Insurance

Ronne, George E.. **Best's Review**. (Property/casualty insurance edition).Oldwick: Apr 1991. Vol. 91, Iss. 12; pg. 74, 3 pgs

» Jump to full text

Subjects:	Disaster recovery, Data integrity, Controls, Computer security, Access control
Classification Codes	Disaster recovery, Data integrity, Controls, Computer security, Access control
Classification Codes	9190 United States, 5220 Data processing management, 5140 Security management
Locations:	US
Author(s):	Ronne, George E.
Publication title:	Best's Review. (Property/casualty insurance edition). Oldwick: Apr 1991. Vol. 91, Iss. 12; pg
Source Type:	Periodical
ISSN/ISBN:	01617745
ProQuest document ID:	216338
Text Word Count	2390
Article URL:	http://gateway.proquest.com/openurl?ctx_ver=z39.88-2003&res_id=xri:pqd&rft_val_fmt=ori:

Abstract (Article Summary)

For insurance executives, as for other business executives, computer security has become a popular topic as reports of computer-related crime continue to mount. Managers should be aware of the security measures that they can take in 4 major control categories: 1. physical security, which deals with the physical protection of the computer operations, 2. data security, which deals with management's measures to establish the necessary degree of protection, 3. applications controls, which help to ensure the accuracy, completeness, and validity of the data processed, and 4. integrity controls, which generally apply to all computer systems and reside to a great extent within the computer operations. According to a Law Enforcement Assistance Administration document, computer-related crime may be committed by the following people: 1. system programmers, 2. computer operators, 3. maintenance personnel, and 4. users. In addition, data processors who provide or handle input data, supervisory personnel, disgruntled employees, and hackers can be involved.

Full Text (2390 words)

Data Security: The Best Insurance

BY GEORGE E. RONNE

For insurance executives, as for other business executives, computer security has become a hot topic as reports of computer-related crime continue to mount. Stories about fraud, destruction and alteration of data, wiretapping,

computer worms, viruses and the like have been published across the country. While some of the reports may seem far-fetched, many, unfortunately, are true. Although such things do happen, and should be guarded against, it is important to remember that simple errors, once in the system, can have just as great an impact on company operations.

To put things in perspective, an executive should assess the economic consequences of a variety of risks. For example, what if:

* Production schedules and/or inventory scheduling were based on inaccurate information?

* Shipments were not billed?

* Computer files or programs were lost?

* The competition gained access to corporate plans, mailing lists or sales data?

* The computer was not available for a week to 10 days?

It is clear from the depth of these problems that control over computer systems is critical. Moreover, security is much too important to place responsibility for it in the hands of a single department like information systems or security. The information services department is a separate support function that has no corporate authority, while the corporate security department may have the authority, but lacks the expertise. Computer security controls, therefore, must come from the top, but before appropriate action can be taken, there must be some perception of the nature, frequency and magnitude of the risks, as well as the controls that are available to counteract these hazards.

The discussion here is designed not to make you an instant data processing security expert, but rather to alert you to the hazards that threaten the security of computer operations and to outline a few areas where prevention should be emphasized.

These controls have been designed to lessen the risk not only of fraud and disaster, but also the risk stemming from error, the primary cause of day-to-day problems that are experienced by the business community. The controls are not all-inclusive, nor should all of them be incorporated into a single system. But managers should be aware of the security measures that they can take in four major control categories: physical security, data security, applications controls and integrity controls.

Physical security deals with the physical protection of the computer operations, including unauthorized entry, personnel policies and damage from fire, water and power failure. It includes a general evaluation of security measures in the computer center, the terminals and the mini- and microcomputers found throughout the organization.

Data security deals with management's measures to establish the necessary degree of protection. The areas include system access, compartmentation, encryption, communications (dial-up/modem) and the instruction of employees in computer-security methods.

Applications controls vary from system to system or application to application. They may reside within or outside the computer operations and help to ensure the accuracy, completeness and validity of the data processed.

Integrity controls generally apply to all computer systems and reside to a great extent within the computer operations. They include the controls over development, use and custody of computer programs and help to ensure the continued operation of the applications controls.

Let's consider who might pose the greatest hazard to computer security. According to a Law Enforcement Assistance Administration document titled "The Investigation of WhiteCollar Crime," computer-related crime may be committed by the following people in any number of ways:

* System programmers can install errors or logical oversights into a program, causing a weak point that can be exploited over and over again. They also can disclose protected measures to outsiders and disable or neutralize protective features.

* Computer operators can tamper with programs, disclose organizational and procedural safeguards and copy files for competitors or other buyers.

* Maintenance personnel can disable protective hardware and use test programs to examine or copy files or alter system programs.

* Users can impersonate others, falsify their own files to deceive others and penetrate the operating system to alter object programs.

In addition, data processors who provide or handle input data, supervisory personnel, disgruntled employees and hackers can be involved in computer-related crime. Let's take a look at the major areas that offer opportunity for implementing security controls,

Physical security. Physical security must be considered as a defense in depth. It involves the establishment of a system of barriers that provides information security to the entire corporation from human and physical threats. A company may not be able to protect its information operation from every threat, but certain risks should be carefully evaluated for any computer center. A 5% cost of the annual budget can be considered a reasonable expense for computer security.

FIRE PREVENTION

Fire. Since fire is one of the more common risks, the installation of a fire alarm system is essential. Passive infrared sensors and dual chamber ionization smoke detection, which evaluate the density of the air caused by smoke, are more effective than devices that measure a rise in temperature. Detectors should be placed throughout the computer center, including above the ceiling and under the raised floor. The system should be connected to the local fire department.

An extinguishing system is needed in addition to the detection system. Generally, halon or a water system can be used. If appropriate steps are taken to shut off electricity, a water extinguishing system will not damage hardware. Halon is an excellent extinguishing agent that causes little or no damage to hardware but raises environmental concerns.

Some insurers use a combination of systems with halon, which is expensive, as the primary agent. A dry- or wet-pipe water system then can be used as the backup. To avoid additional problems, it is important to provide for the removal of water.

Hand-held extinguishers are extremely important in reducing the fire hazard and should be placed throughout the computer center. Several alarm switches and protected power switches also should be accessible. In addition, all equipment must be maintained in working order. Emergency lighting must be in place, and employees must know what to do when fire occurs. Additionally, the computer room must be cleaned regularly, including the space that is under the computer-room floor.

It is important to include the areas adjacent to the computer center in a fire prevention program. Too often, the fire that causes damage starts in an adjoining area, around, above or below the computer center. In addition, all electrical work must be done by a licensed electrician.

THE BEST INSURANCE

An emergency plan is essential. Consider a disaster recovery plan not only for MIS, but for the entire company. The development of the plan, the training of personnel and the testing and maintenance of the plan may be the best insurance a company has.

Water damage. Construction features can help to avoid damage by water. The computer center should not be located in a basement. If severe storms or hurricanes pose a threat, the center should be constructed without windows. If windows are installed, they must be able to withstand high winds.

In the building design, it is important that all plumbing be routed around the computer center, including the area above it. If a sprinkler system is installed, a time delay and alarm that permits manual cutoff will prevent accidental damage. The area must have floors that permit quick drainage.

Power/air conditioning failure. The damage caused by power failure generally is less serious than that from other hazards, but precautions should be taken to prevent a system shutdown. The impact of a shutdown should be evaluated when designing the system's backup. The effects of transients and brownouts can be avoided by the use of special electric equipment, and the effects of a power outage can be eliminated by an on-site generator or battery

bank. The power requirements of mini- and microsystems throughout the company must be included in the security plan.

To prevent a shutdown caused by improper levels of temperature and humidity, the air conditioning system must be in good order.

DETECTING INTRUDERS

General physical security. Most companies will not find it necessary to install an extensive intrusion detection system, but certain devices are appropriate for many. Current systems include microwave, ultrasonic, passive infrared and balanced magnetic switches. Closed circuit television and security guards are common. One or a combination of these elements might be appropriate, depending on the desired degree of control.

Vulnerability to sabotage has increased because computers and terminals are located throughout the company. Many companies employ a badge system to limit access to the computer center and other sensitive areas. Access control is the key, and people who are not employees have no business in the computer center. If access is essential, an employee who knows what the visitor is doing must monitor that person in the center. The computer system is the bank vault of a corporation and should be treated as such.

Personnel. Without a doubt, one of the most important aspects of any computer security program is the dependability of the people who have access to it. A dishonest employee can do far more harm than an outsider. Management must conduct an adequate investigation when an individual is hired and monitor changes throughout that employee's career with the firm.

Backup protection. Regardless of how tight security measures are, backup protection must be in place at every personal computer. The operating system, application programs, documentation and current critical files must be backed up. In most cases, a vendor can replace hardware, but without the backup, there is nothing to run.

To protect backup files adequately, they should be stored off site. The off-site location must be inspected regularly and should not be subject to the same disasters that might hit your location. Once the storage site is selected, it is important to rotate files to ensure that you have what is necessary.

Data security. Many of the basic procedures found in a viable computer security program will give a significant degree of protection against most security problems. The need for strong senior management support of the program is essential, and the appointment of an individual responsible for the program will foster the implementation of an effective and well-founded computer security system. The key is to identify the areas that require protection and to concentrate on them. Trying to protect everything will detract from your efforts.

The computer security manager must be a teacher, a coordinator and an enforcer. The manager must make people aware of the need for the program and make sure they know the part they play in the effort. The effort must be coordinated with the users and managers, and the managers must be responsible for their part in the overall effort. The computer security manager must be responsible for the establishment and enforcement of corporate policy, including access control and employee education.

UNAUTHORIZED ACCESS

Applications controls. These controls are designed to prevent errors in data input, conversion, unauthorized input or manipulation, and unauthorized access to data. Unauthorized access and manipulation are probably the most serious threats.

Most computer-assisted fraud results from a lack of proper control over data input. In many cases, more than one control weakness, such as inadequate control over **transaction** input coupled with improper division of duties, can result in misuse of data. Controls over data input and other applications controls will prevent the entry of unauthorized data. This is important to all systems, but especially to on-line systems, because they often can be accessed from a remote location through a telephone line. Appropriate safeguards must be placed on the mainframe system and on personal computers throughout the company. Hardware or software controls must limit access to computer files to those who are authorized. Smart **cards** and **biometric** devices help to control access to computer systems and hardware.

PASSWORD PROTECTION

In facilities where passwords are system-generated and changed at frequent intervals, they provide good security.

In other facilities, their usefulness is negated by writing the password on the side of the terminal, software that prints out the password, or lack of control over the distribution of the password.

A computerized log of all those who gain access, as well as attempts at access, is advisable. The use can then be reviewed for unusual events like an increase in the number or size of transactions from a certain terminal or transactions from a terminal during hours when a department is not in operation. Many systems will automatically shut down a terminal after a predetermined number of unsuccessful attempts to log onto the system. After a specific period of inactivity, a system should not allow a transaction until a required password is provided.

Input. A system should contain controls that ensure the completeness and accuracy of input data. Problems may occur in production with the entry of an inaccurate amount or code or from incomplete input. One-for-one checking, batch totals, sequence checks, matching, programmed checks and prerecorded input can help eliminate input errors.

Processing. The control techniques that apply to input generally apply to the processing system as well, including updating files. The controls previously listed can ensure that all files have been processed. Specific controls must be used to ensure that data is properly processed and that all data is valid. Validity checks should be programmed into the system. The planning and execution of maintenance is essential and must not be overlooked. Security controls here are as vital as anywhere else in the corporate computer security program.

OUTPUT PROTECTION

Output. Many controls over access, accuracy and completeness of data have been established, but it is essential that all printed and magnetic output be given the same degree of protection. Authorization tables that identify who may read, write or edit data are helpful. Unless controlled, data output can often negate that effort. Some batch jobs, when printed, contain the password and are handled in a manner that permits access by unauthorized individuals.

While risks are present in any system, the most significant problem is simple error. Management must ensure that operating personnel are aware of the importance of accuracy and completeness of information and take steps necessary to ensure the security of the system. The entire organization depends on it.

GEORGE E. RONNE, CPP, is a senior consultant with M&M Protection Consultants, St. Louis.

---

^ Back to Top « Back to Results < Previous Article 5 of 9 Next > Publisher Information

Print Email ☐ Mark Article Abstract , Full Text , Page Image - PDF

Automated fingerprint analysis offers fast verification

Hollingum, Jack. **Sensor Review**. Bradford: 1992. Vol. 12, Iss. 3; pg. 12, 4 pgs

» Jump to full text

Subjects:	Security systems, Product development, Product design, Electronics industry, Case studi
Classification Codes	Security systems, Product development, Product design, Electronics industry, Case studi
Classification Codes	9175 Western Europe, 9110 Company specific/case studies, 8650 Electrical, electronics, i
Locations:	UK
Companies:	Printscan Verification
Author(s):	Hollingum, Jack
Publication title:	Sensor Review. Bradford: 1992. Vol. 12, Iss. 3; pg. 12, 4 pgs
Source Type:	Periodical
ISSN/ISBN:	02602288
ProQuest document ID:	1310033
Text Word Count	1824
Article URL:	http://gateway.proquest.com/openurl?ctx_ver=z39.88-2003&res_id=xri:pqd&rft_val_fmt=ori:

Abstract (Article Summary)

A biometric system based on the well-established approach of fingerprint identification, but avoiding both the heavy data demand and the doubtful social acceptability associated with an actual fingerprint record, is gaining widespread interest. The technique extracts certain key features from a fingerprint or other friction ridge skin pattern and compresses them into only 918 data bits - small enough to be written into tracks one and 3 of an ISO standard magnetic stripe card. It is not possible to reconstruct a fingerprint from the data. Assisting acceptance of the system is the fact that its developer, Brendan Costello, worked on it in close collaboration with the police. It is based on a technique known as coincident sequencing, which has been used by police fingerprint experts for nearly 100 years and operates up to full national or international fingerprint law standards. Costello has assigned the patents covering the system to his company, Printscan Verification Systems, with subsidiaries in the UK and the US. A developement system has been built, as well as a briefcase-sized portable demonstration system that is used in presentations to prospective licensees.

Full Text (1824 words)

Widespread interest is being shown in a biometric system based on the well-established approach of fingerprint identification, but avoiding both the heavy data demand and the doubtful social acceptability associated with an actual fingerprint record. The technique extracts certain key features from a fingerprint or other friction ridge skin pattern and compresses them into only 918 data bits--small enough to be written into tracks one and three of an

150 standard magnetic stripe card. It is not possible to reconstruct a fingerprint from the data.

Assisting acceptance of the system is the fact that its developer, Brendan Costello, worked on it in close collaboration with the police. It is based on a technique known as "coincident sequencing" which has been used by police fingerprint experts for nearly 100 years, and operates up to full national or international fingerprint law standards.

Costello has assigned the patents covering the system to his company, Printscan Verification Systems, with subsidiaries in Britain and the USA. A development system has been built, and in addition a briefcase-sized portable demonstration system has been developed and is used in presentations to prospective licensees (see photograph). In April of this year it won the company the Silver Medal at the 20th International Exhibition of Inventions in Geneva. The system was also demonstrated at the Hanover Fair in April on the stand of Eltec Elektronik, which supplied the image processing board. One licence for the system has been awarded to a South African company for a security application, and a number of other negotiations are in progress, most notably in Japan.

The potential scope of applications is very wide indeed. They can be broadly divided into financial applications and access control. Inadequate security of the ordinary PIN system for credit and charge **cards** has resulted in attempts to find more reliable methods of identification, some of which require the memory and computing facilities of a smart **card**. The Printscan record, totalling only 918 bits, can easily be held within a standard magnetic stripe, making it an attractive possibility for automatic teller machines, credit and charge **card** identification in stores, computer financial **transactions** and other situations where it is vitally important to prevent fraud. But it is not only accuracy which is required in large-market applications. The **biometric** system must also be simple, cost-effective and user friendly. On all of these counts the new system appears to have much to recommend it.

Access control is needed in many situations, and complicated precautions are taken where high security is required. The Printscan method is quick, inexpensive, reliable, and does not invade privacy or raise questions of civil rights. For access to secure buildings, a computer network or other situation where a number of people are allowed exclusive access, each person's fingerprint scan could be compared to a stored bank of scans held in an on-line database. Similarly a centralized database system for a hotel could grant access for individuals to particular room numbers.

On passports, driving licences, identity cards and so on, a scan, together with a magnetic record on the document, would verify the identity of the document holder. The system could even be used to give access to vehicles and in vehicle ignition systems by storing the coded data in on-board memory on the vehicle and granting access only with a valid fingerprint.

The only image" of an individual's fingerprint is the skin pattern on his/her own finger. As soon as the key features are extracted from a scan for encoding, the scanned electronic image is discarded. The information stored on the magnetic stripe card, in PROM or in a database, is of no significance except in association, simultaneously, with a scanned image of the finger. Again, as soon as verification is complete the image is discarded. Sophisticated methods may be built into the system to counter enforced presentation.

The business policy of Printscan Verification Systems is to market the technology by means of licensing agreements to major corporations and institutions associated with the security and finance sectors--either nationally or internationally. The company is also able to assist with or undertake design and development contracts for work specific to an end-user, on behalf of interested parties.

To date, patents have been fully granted in the USA and Australia. The European patent has been approved by the EPO and formal grant is imminent. Patents are pending in Japan and the Confederation of Independent States (formerly the USSR).

SCAN EQUIPMENT

The development system has been built for Printscan by Essex Electronics Consultants, a wholly owned subsidiary of the University of Essex, and is being used not only to carry out development work but also to provide a general demonstration capability based on a scanner, processing unit and magnetic card stripe reader/writer. It is shown diagrammatically in Figure 1. (Figure 1 omitted)

The system incorporates a solid-state fingerprint scanner developed by the Industrial Physics Group at the University of Essex. It uses low-cost components, and is suitable for a wide range of applications, from bank cash-dispensing machines to all levels of access control and identification systems. It is the subject of a separate

patent application. The scanner supplies image data to the processing unit, which incorporates an Eltec IC4O image processing board. Processed data from the image can be written to and read from a card reader/writer unit for encoding and verification.

Essex Electronics Consultants has also built a portable demonstration unit (see Figure 2) using off-the-shelf components, which can be taken to potential clients to demonstrate the system's encoding and verification processes. (Figure 2 omitted)

The software algorithms used in carrying out the coincident sequencing operation on the fingerprint scan are held in EPROM, allowing the encoding of data into a magnetic stripe and the verification of a fingerprint to be carried out very rapidly. Verification of a fingerprint scan is completed in one to two seconds if a match can be found with the fingerprint data on the magnetic stripe card. Rejection of an incorrect fingerprint takes a little longer. Accurate measurements of error rates have not yet been obtained, but tests are under way to establish these, which are expected to be very low.

COINCIDENT SEQUENCING

Coincident sequencing has been used by police forces as a manual method of fingerprint identification for many years. The Printscan technique automates the task. It ignores the major fingerprint features of arch, loop and whorl and concentrates attention on the "minutiae"--the points where ridges end and where they divide (bifurcate), looking at the relationships between a number of these features. The coincident sequence is defined by:

* the type of feature (ridge end or bifurcation)

* the position of the feature relative to other features in the group being processed

* the orientation of the feature relative to others in the group being processed

* the count of ridges lying between each feature and every other feature in the group.

To simplify the analysis the scanned image is first processed to make identification of features easier. The original grey-scale image (Figure 3 (a)) is first filtered to create a cleaned black-and-white image (Figure 3 (b)), and goes through a process of edge extraction so that pores and other irregularities are ignored (Figure 3 (c)). Finally the image is thinned to a single pixel width for each ridge (Figure 3 (d)). Several criteria are employed in the automatic selection of a set of features, including the reliability of each feature, the presence of an adequate number of ridges between the feature and each of the others selected, a satisfactory angular variation to ensure covering an area of the print, and a satisfactory mix of ridge ends and bifurcations. A typical image with six features marked on it is shown in Figure 4. (Figure 4 omitted) Ridge ends are indicated with circles and bifurcations with squares.

For representation in a magnetic stripe card the information must be presented in data bits. The two types of features can be distinguished by one data bit per feature. The processed image is held in a grid of 512 by 512 pixels (see Figure 4 (a)) so the position of each feature can be defined by its pixel count in each direction. This requires nine bits for each axis or 18 bits for each feature. Angular relationships between the orientations of features are defined in terms of eight "compass points" (see Figure 4 (c)) needing another three bits for each feature. The orientations of eight features are shown in Figure 4 (e).

Up to 16 ridges are allowed between features, requiring four bits for each connecting line. Figure 4 (d) shows how the counts are taken for eight features. In general the total number of bits used to identify N features is: (Equation omitted)

A table covering these characteristics for six features is shown in Figure 4 (b).

For a coincident sequence to exist there must be at least four features in the set to be inspected, and preferably at least one feature should be of a different type from the others. For criminal identification purposes, fingerprint experts use 16 features in coincident sequence in the UK. In France 17 features are required, but in the rest of the world 12 features are considered adequate for criminal identification. For civilian use, eight features in coincident sequence are generally accepted as sufficient.

Even with a full analysis of 17 features, the number of data bits required to record all the information is only 918. A standard magnetic stripe card has three tracks of which the second is used in automatic teller machines. The first and third tracks are less widely used and have a total capacity of 1,088 data bits--more than adequate for a 17-feature fingerprint record, so this number of features has been selected as the most convenient for entry on a

magnetic stripe card.

VERIFICATION

A similar procedure is followed in comparing a person's fingerprint with the record on the magnetic stripe card. The print is scanned, and all the reliable ridge ends and bifurcations are identified--which may be many more than 17. The relevant data for each feature (type, location, orientation and number of ridges to each other feature) are calculated, and this process continues until eight points of similarity are found between these features and those recorded on the magnetic stripe card. If eight points of similarity cannot be found, verification is refused.

With 17 features covered in the magnetic stripe record, there is a large measure of redundancy in the information, since only eight correspondences are required. This allows for any changes which may have occurred to a finger, such as a cut or abrasion, or dirt between the ridges. The software also incorporates adjustments of translation and rotation to the feature locations to allow for the fact that the finger may be placed differently on the scanner.

Printscan Verification Systems can be contacted at 89 High Street, Hadleigh, Ipswich, Suffolk IP7 5EA. Tel: 0728 79553; Fax: 0728 79276.

---

^ Back to Top « Back to Results < Previous Article 3 of 9 Next > Publisher Information

Print Email ☐ Mark Article Abstract , Full Text
